8-28-2017

Many-particle Systems, 11

David Peak
Utah State University, david.peak@usu.edu

Many-particle Systems, 11

Quantum information

In Mn10 we discussed the rudiments of "classical computation." Classical, conventional computation involves combinations of transistors that convert low- and high-voltage inputs into different low- and high-voltage outputs. These voltages are interpreted as the **b**inary dig**its** 0 and 1, i.e., as *bits*. How bits are changed into other bits leads to such things as text preparation and storage, numerical calculations and symbolic manipulations, image and sound generation, game playing, intercontinental communication—in short, the modern world of information.

Transistors work as a result of the quantum mechanics of electronic wavefunctions and their associated energy bands. On the other hand, the voltages that define bits are determined by just the number of electrons on what are effectively microscopic capacitor plates, not by the electrons' wavefunctions. In this sense, bits are classical; they are not infected with quantum uncertainty (though they might be altered by thermal fluctuations or energy jolts from cosmic ray collisions; in fact, such bit "errors" occur all the time in conventional computers and a substantial fraction of a computer's processing activity is devoted to detecting and correcting such errors).

The *processes* that transform bits in conventional computers are similarly classical. A typical logic gate in a conventional computer has multiple inputs and fewer outputs. For example, an AND gate has two inputs and one output. It converts two bits into one. One bit of information is "lost" in the AND process. A consequence of this is that AND is not reversible: if the one out-bit is 0, the two in-bits could equally likely be 01, 10, or 00; it is impossible to tell which. In classical *irreversible* dynamical systems mechanical energy is "dissipated," that is, converted into thermal energy. That occurs in conventional, classical computers, too. The energy of the bits that are lost in irreversible processing shows up as heat. That's why conventional computers are hot.

A much discussed and actively researched alternative to classical computing deals with "quantum information." Instead of classical bits whose states are surely either 0 or 1 before they are measured, a quantum computer uses states that are superpositions of both 0 and 1 and only take exact values after a measurement is made. These states are **qu**antum **bits**—qubits ("kew bits"). The prototypical qubit object is a particle with spin-1/2, the direction of which can be "up" (1, say) or "down" (0). Until a measurement of the spin direction is made, the associated wavefunction is a superposition of the up and down possibilities: $\Psi = a\Psi_1 + b\Psi_0$ (a and b are complex numbers such that $|a|^2 + |b|^2 = 1$).

In quantum mechanics, a "legal" wavefunction can be transformed into another "legal" wavefunction by a "unitary transformation." A unitary transformation changes the a and b values, for example, but preserves $|\Psi|^2$. Importantly, *unitary transformations are reversible*. In a quantum computer, the gates that transform qubits into new qubits have to be designed to be reversible: they have to attach extra qubits to the output so that the number in equals the number out. When that is so, no qubits are lost and no heat is generated in the processing. Cool (literally). The extra qubits required by the

quantum gate uniquely identify each output with a corresponding input. In quantum language, the output is "entangled" with the input.

To help clarify the difference between classical and quantum computing let's consider a specific example: the "AND problem." We know that classically AND converts two bits of input (00, 01, 10, and 11) into one bit of output, but we don't know which. To solve the problem classically, we pass each possible input through an AND gate and record the resulting output. This entails four separate actions. In the quantum version, we prepare an initial wavefunction in a superposition of the four possible input states: $\Psi = a_{00}\Psi_{00} + a_{01}\Psi_{01} + a_{10}\Psi_{10} + a_{11}\Psi_{11}$. We pass this state through a quantum AND gate (a qAND gate) that transforms the input wavefunction into an output wavefunction that similarly has four superposition coefficients, each of which (because of the added bits) is uniquely connected to the input coefficients. Thus, in one pass, the qAND gate takes in all possible inputs and produces all possible (correct) outputs. Sounds great, right?

Well, not so fast. In order to record the results, the output wavefunction has to be collapsed into its various pieces by measurements—a minimum of four, in this example. So, there isn't any improvement over classical computation in terms of the number of processing trials. And the apparent savings in heat generation isn't right either: the act of collapsing the wavefunction destroys bits and produces a subsequent little burst of heat! So, what's the big deal then?

It turns out that there are some very hard problems that can take advantage of another aspect of quantum wavefunctions: interference. In these problems, quantum destructive interference allows many otherwise fruitless attempts to get an answer to the problem of interest to be automatically excluded. The result is that quantum computing leads to a *very significant speed up* over classical computing in generating possible answers to the problem of interest. Identifying which problems for which this is true, and how important they are, is a major area of contemporary research. And then there are the, to date, unresolved issues of how to actually make and program such a computer.

The decryption problem

Electronic data security—involving, for example, private personal information, financial resources, election results, or military secrets—is one of the most important challenges facing contemporary society. In general, data security revolves around encryption and decryption. *A* wants to send *B* a message, *M*, that no evil interceptor, *I*, can understand. To do this *A* encrypts the message as $C = E(M)$, where *E* is an encryption rule. Provided *B* knows how to decrypt *C*, *B* is able to read $M = D(E(M))$, where *D* is the appropriate decryption rule. Typically, the encryption and decryption rules change on a regular basis. In order for *A* and *B* to communicate properly and keep *I* from figuring out what is going on, *A* not only transmits *C* but also a key, *k*, that tells *B* what that day's *D* should be. But, this has to be done in a sufficiently sneaky way that *I* doesn't have enough time to catch on before *B* can act on the decrypted message. Numerous algorithms have been produced to do all of this. The most robust of these involve some arcane arithmetic that starts with two long integers (maybe a few hundred digits long), *p* and *q,* that are prime numbers (i.e., divisible only by 1 and by themselves) that are multiplied together. This huge product is one of the pieces of information sent along with the encrypted message. The encryption and decryption depend on the

values of the two prime factors. If *I* can find the factors *p* and *q* quickly enough, *I* can decode the message and do something nasty. This whole procedure works because classical algorithms for finding the prime factors of a whopping big integer take a bloody long time to implement with contemporary computers.

Enter quantum computers. There is a slick quantum algorithm (*Shor's Algorithm*) that, in principle, can find prime factors much faster than any classical method. It does so by taking advantage of quantum destructive interference. To crack the decryption problem for current encryption procedures using Shor's Algorithm, however, requires a largish quantum computer—none of which yet exist. So your bank account is still secure, for now, at least.

The status of quantum computers

Work in numerous laboratories around the world endeavors to produce functional quantum computers that can solve problems no conventional, classical computer can. The hurdles these scientists and engineers are trying to overcome are *how do you create superpositions of large numbers of qubits in the input state* and *how do you preserve entanglement of the qubits through the processing phase so that the output can be uniquely identified with the corresponding input*. Practically every day new progress is reported, often in public media releases before careful technical review has been completed. At this moment (summer 2017), the largest primitive quantum computers have about 20 qubits of input and entanglement persists for microseconds. (These prototypes solve problems, like factoring integers, that ordinary computers can also easily do. So again, no big deal—yet.) The holy grail of quantum computing research is to achieve 50-100 input qubits and retain entanglement for at least minutes. Should this situation be achieved it will signal "quantum supremacy," the ability of quantum computers to outperform the largest and fastest classical computers–at least for certain classes of problems. It is often predicted this will occur in 5 years or so.

A central player in the quantum computer game is the Canadian company, D-Wave. D-Wave first announced a "quantum computer" in 2007 and showed off in several venues things it could do (including solving Sudoku puzzles). Critics agreed that this first device couldn't actually do anything an ordinary computer could. Undeterred, D-Wave has been systematically producing bigger and better devices (none of which have yet unambiguously passed critical scrutiny), claiming at present to have a 1000 qubit machine! Because of D-Wave's erratic history there are many skeptics of their claims. (See, e.g., Scott Aronson's continuing blog posts at http://www.scottaaronson.com/blog/. Also, it helps to keep up with quantum computing developments by reading the MIT Technology Review at https://www.technologyreview.com.) Nonetheless, Google and NASA have purchased a D-Wave computer (for $10,000,000!) to use in their collaborative Artificial Intelligence Laboratory, so maybe the hype is real. Who knows?

We live in a brave new, quantum mechanical, world.